



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,445	10/31/2001	Richard Paul Tarquini	10016861-1	2406

7590 03/22/2005

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 03/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

10/001,445

Applicant(s)

TARQUINI ET AL.

Examiner

Samson B Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 October 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date Jun 18, 2003.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

Art Unit: 2132

## ***DETAILED ACTION***

1. **Claims 1-12** have been examined.

### ***Preliminary Amendment***

2. The preliminary amendment, submitted and requested for consideration by the applicant is acknowledged. The office action has been written after the submitted preliminary amendment is taken in to consideration.

### ***Drawings***

3. The drawing is objected to because of the following informalities.
  - Figure 2, ref. Num “80” and “81”, which is recited as “Network based IPS “ on the disclosure is designated as “**Network IDS**”. Even though, they meant to be one and the same thing, figure 2, ref. Num “80” and “81” has to be corrected as “**Network IPS**” to be consistent to the disclosure.

Appropriate correction for the drawing (Figure 2) is required.

### ***Claim Objections***

4. Claim 8 is objected to because of the following informalities.

Art Unit: 2132

Claim 8, recites “binding the network filter service provider to a protocol driver **a the** network stack of the node.” It should be corrected as “binding the network filter service provider to a protocol driver **of a** network stack of the node.”

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 8-12** are rejected under 35 U.S.C. 102(e) as being anticipated by **Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061)

7. **As per claims 8 and 11**, **Holland discloses a method of performing intrusion prevention** [figure 1, ref. Num “20”, ref. Num “19”, ref. Num 18”] **at a node** [figure 1, ref. Num “11” ref. Num “12”] **of a network** [figure 1, ref. Num 10], **comprising:**

- **Binding a network filter service provider** [figure 2, ref. Num “37”] **to a media access control driver of a network stack of the node** [figure 2, ref. Num “31”; column 4, lines 53-57] (The MAC driver is inherently included in the NIC. The MAC or the “media access control driver”, also called the “network card driver”, allows the operating system

Art Unit: 2132

to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC); and

- **Binding the network filter service provider** [figure 2, ref. Num “37”] **to a protocol driver of a network stack of the node.** [Figure 2, ref. Num “33” or figure 3, ref. Num “52”; and figure 4, ref. Num “82” and ref. Num “83”; Column 6, lines 27-31](The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num “82”, “83” are implemented by software drivers which are also called protocol drivers. Binding is the process of associating two pieces of information with each other. With respect to **Holland** the Packet filter service which is shown on figure 2, ref. Num “37” is binding to both the MAC driver which is inherently included in the NIC and the Packet filter is also binding to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num “33” and shown also on figure 3, ref. Num “52”. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num “82” and “83”, namely the network layer and the transport layer are all implemented by the protocol driver.) **[For the definitions that the examiner used, see the reference U)**

Art Unit: 2132

8. **As per claim 9, Holland** discloses the method of performing intrusion prevention as applied to claim 8 above. Furthermore Holland discloses the method further comprising filtering, by the network filter service provider, all data received by the media access control driver prior to passing of the data to the protocol driver. [Figure 2, ref. Num “37” and ref. Num “33”; column 4, lines 41-43] (All data received by the media access control driver which is inherently included in the NIC shown on figure 2, ref. Num “31” is filtered by the packet filter shown on figure 1, ref. Num “37” before it reaches the IP Stack which is inherently includes the protocol driver, since the IP layers namely the network layer shown on figure 4, ref. Num “82” and the transport layer shown on figure 4, ref. Num “83” are all implemented by the protocol driver. This filtering is done when the incoming data frame is eventually delivered to the host application )

9. **As per claim 10, Holland** discloses the method of performing intrusion prevention as applied to claim 8 above. Furthermore Holland discloses the method further comprising filtering, by the network filter service provider, all data received by the protocol driver prior to passing of the data to the media access control driver.[Figure 2, ref. Num “37” and ref. Num “31”; column 4, lines 43-48](Out going data packets originating from the host application shown on figure 4, ref. Num “40” are processed through the IP stack are filtered as shown on figure 2, ref. Num “37” and eventually transmitted through the MAC which is inherently included in the NIC shown on figure 2, ref. Num “31”)

10. **As per claim 12, Holland** discloses the method of performing intrusion prevention as applied to claim 8 above. Furthermore Holland discloses the method wherein binding the network filter service provider to the media access control driver and to the protocol driver occurs upon initialization of the operating system. [Figure 1, ref. Num “32”, ref. Num “31” ref. Num “33” and ref. Num “37”]

### ***Claim Rejections - 35 USC § 103***

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. **Claims 1-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Holland III et al** (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061) in view of **Douglas B.Moran**, (hereinafter referred to as **Moran**) (U.S. Patent No. 6,826,697)

13. **As per claim 1, 4 and 7**, **Holland** discloses a **node** [figure 1, ref. Num "11" ref. Num "12"] of a **network running an intrusion detection system**, [ Column 1, lines 15-18; figure 1, ref. Num "20", ref. Num "19", ref. Num 18"] (The present invention relates in general to network intrusion detection data collection and, in particular, to a system and method for intrusion detection data collection using a network protocol stack multiplexor). **The node comprising:**

- **A central processing unit;** [ Column 4, lines 20-23]
- **A memory module for storing data in machine readable format for retrieval and execution by the central processing unit;** [Column 4, lines 23-29]

Art Unit: 2132

- **A database for storing a plurality of machine-readable network-exploit signatures; [Column 4, lines 5-8; figure 1, ref. Num “20” or “Hybrid IDS”]**  
(As shown on figure 1, The network IDS 18, host IDSs 19, and hybrid IDS 20 all collect and analyze a traffic stream to detect any attempts or actual compromises of network or system security. The network IDS 18 focuses on all traffic entering the intranetwork 18 and analyzes that traffic using signature-based and statistical-based intrusion detection techniques meets the limitation of the “a database for storing a plurality of machine-readable network-exploit signatures”.)
- **An operating system** [Figure 2, ref. Num “Kernel”] ( The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**  
  
**A network stack comprising a protocol driver,**[Figure 1, ref. Num “33”; figure 3, ref. Num “52”; figure 4, ref. Num “82” and ref. Num “83”; Column 6, lines 27-31 ] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num “82”, “83” are implemented by software drivers which are also called protocol drivers)
- **A media access control driver** [figure 2, ref. Num “31”; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the “media access control driver”, also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The



Art Unit: 2132

MAC driver got its name from the fact that it operates at the lower level of the OSI model. The second layer of the model, the Data Link layer, is divided into two pieces: the LLC and MAC. The LLC sub layer is implemented in the transport driver while the MAC sub layer is implemented in the NIC) and

• **An instance of the intrusion detection system implemented as an intermediate driver [Figure 2, ref. Num “37”] and bound to the protocol driver [figure 2, ref. Num “33”] and the media access control driver.**[figure 2, ref. Num “31”] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num “37” is implemented as an intermediate driver and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num “33” and shown also on figure 3, ref. Num “52. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num “82” and “83”, namely the network layer and the transport layer are all implemented by the protocol driver.)

**Holland** does not explicitly discloses

- A database for storing a plurality of machine-readable network-exploit signatures;

However, in the same field of endeavor, **Moran** discloses a database for storing a plurality of machine-readable network-exploit signatures; [Column 8, line 5; figure 3, ref. Num “308”]

Art Unit: 2132

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of having an attack signatures database as per teachings of **Moran** in to the method analyzing the traffic using signature-based and statistical-based intrusion detection techniques as taught by **Holland**, in order strengthen the security by providing an improved system and method for detecting computer intrusions. [See Moran column 3, lines 18-20] **[For the definitions that the examiner used, see the reference U)**

14. **As per claim 2**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 1 above. Furthermore Holland discloses the method wherein ,a frame received on a network medium connected to the node [figure 2, ref. Num "13"] is processed by the media access control driver,[figure 2, ref. Num "31"] the intrusion detection system [figure 2, ref. Num "37"] receiving the processed frame directly from the media access control driver.[figure 2, ref. Num "31"]

15. **As per claim 3**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 2 above. Furthermore Holland discloses the method wherein the intrusion detection system receiving the processed frame is operable to pass the processed frame to the protocol driver.[Figure 2, ref. Num "37" and ref. Num "33"; Column 4, lines 41-43] ] (All data is filtered by the packet filter shown on figure 1, ref. Num "37" before it reaches the IP Stack which is inherently includes the protocol driver, since the IP layers namely the network layer shown on figure 4, ref. Num "82" and the transport layer shown on figure 4, ref. Num "83" are all implemented by the

Art Unit: 2132

protocol driver. This filtering is done when the incoming data frame is eventually delivered to the host application)

16. **As per claim 5**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 1 above. Furthermore Holland discloses the method wherein, a datagram generated by the node is received by the intrusion detection system.[figure 2, ref. Num "37"; column 4, lines 57-58]

17. **As per claim 6**, the combination of Holland and Moran discloses the method of intrusion detection as applied to claim 5 above. Furthermore Holland discloses the method wherein, the intrusion detection system is operable to pass the datagram to the media access control driver. [Figure 2, ref. Num "37" and ref. Num "31"; column 4, lines 43-48; column 4, lines 52-58](Out going data packets originating from the host application shown on figure 4, ref. Num "40" are processed through the IP stack and filtered as shown on figure 2, ref. Num "37" and eventually transmitted through the MAC which is inherently included in the NIC shown on figure 2, ref. Num "31")

### ***Conclusion***

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

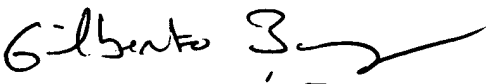
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone

Art Unit: 2132

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA  
**S.L.**  
03/09/2005

  
GILBERTO BARRÓN JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100